Position statement
ICSE'99 Panel on Survivable Systems
Dr. Robyn R. Lutz

Experience with robust, safety-critical systems offers some approaches to meeting four key challenges in the development of survivable systems:

(1) Evolving requirements. One of the most difficult aspects of engineering a survivable system is the degree to which the requirements for survivability relentlessly evolve during the system's development. Survivability requirements change with advances both in defensive measures and in threats. Component-based development, with reuse of product families where appropriate, supports rapidly evolving systems.

(2) Design trade-offs. The design of survivable systems involves difficult trade-offs. For example, certifiable COTS components with formally specified interfaces enhance the predictability of composed behavior. However, the lack of diversity in reusable components may increase the system's openness to attack. Explicit requirements negotiations among stakeholders and explict documentation of operating assumptions and limits of survivability assist in trade-off decisions.

(3) Adequate hazards analysis. For survivable systems, hazard analysis can reduce performance risk and help structure the on-going process of refining and prioritizing the survivability requirements. As with many safety-critical systems, some hazards cannot be avoided or prevented, but must be handled through additional fault monitoring and recovery software, increasing complexity. Software failure modes and effects analysis and software fault tree analysis enhance understanding of interactions and of the contributing causes of hazards.

(4) Verification of new architectures. Architectures that support change and facilitate maintenance are essential to survivable systems. However, these architectures are inadequately tested by traditional verification techniques. Formal methods offer a way to begin modeling and investigating the behavior of the planned system, and to validate that key properties hold invariantly in the system as modeled.